Max Planck Institute for Innovation and Competition Research Paper No. 18-24

Peter Georg Picht and Gaspare Tazio Loderer

Framing Algorithms – Competition law and (Other) Regulatory Tools

Max Planck Institute for Innovation and Competition Research Paper Series

Framing Algorithms – Competition law and (Other) Regulatory Tools

Peter Georg Picht,[*] *Gaspare Tazio Loderer*[**]

***Abstract**: As other fields of law, competition law is put to the test by new technologies in general and algorithmic market activity in particular. This paper takes a holistic approach by looking at areas of law, namely financial regulation and data protection, which have already put in place rules and procedures to deal with issues arising from algorithms. Before making the bridge and assessing whether the application of any such tool is fruitful for competition law, the paper discusses important competition cases regarding algorithms, including the Google Shopping, Lufthansa and Facebook case. It concludes with some policy recommendations.*

***Keywords**: Algorithms, Artificial Intelligence, Competition Law, Regulation, algorithmic trading, high-frequency trading (HFT), General Data Protection Regulation (GDPR), algorithmic collusion, big data, Google Search (Shopping), EU Commission, Lufthansa, Bundeskartellamt, Facebook*

***Abstract**: Auch das Kartellrecht wird durch neue Technologien, insbesondere durch algorithmische Handelsaktivität, auf die Probe gestellt. Durch Vergleich mit anderen Rechtsgebieten, die bereits Regeln im Hinblick auf die durch Algorithmen resultierenden Herausforderungen erlassen haben, wie das Finanzmarktrecht und Datenschutzrecht, verfolgt dieser Beitrag einen holistischen Ansatz. Bevor die Frage aufgeworfen wird, ob die in anderen Rechtsgebieten eingesetzten Tools auch für das Kartellrecht fruchtbar gemacht warden können, werden wichtige kartellrechtliche Entscheidungen mit Algorithmenbezug angerissen, inkl. Google Shopping, Lufthansa und Facebook. Der Beitrag endet mit regulatorischen Empfehlungen.*

***Schlagworte**: Algorithmen, Künstliche Intelligenz, Kartellrecht, Regulierung, algorithmischer Handel, Hochfrequenzhandel, Datenschutz-Grundverordnung (DSGVO), Kollusion, Big Data, Google Search (Shopping), EU Kommission, Lufthansa, Bundeskartellamt, Facebook*

[*] Professor Dr, LL.M. (Yale), Chair for Business and Commercial Law, Center for Intellectual Property and Competition Law—CIPCO, University of Zurich; Affiliated Research Fellow, Max Planck Institute for Innovation and Competition, Munich.

[**] MLaw, Attorney-at-Law, PhD-Candidate and Research Assistant to Professor Dr Peter Georg Picht.

1. Introduction

'*Success in creating AI would be the biggest event in human history. Unfortunately, it may also be the last, unless we learn how to avoid the risks*'.[1]

Two pricing algorithms, competing to sell a genetics textbook, strategized their interaction so 'cleverly' that they ended up – not quite – selling the book for USD 23 million a copy.[2]

Although competition law may not be among the first topics one associates with algorithms[3] or Artificial Intelligence (AI)[4], it is certainly one area of law that starts to take a closer look at the phenomenon, and rightfully so. The use of algorithms does not only present great chances to economy and society, it can also lead to undesirable results, on a large and a small scale. The algorithms used today can be surprisingly low in their level of sophistication. However, as they become more complex and move towards an 'intelligent' state, they are likely to disruptively change almost all areas of human life. Even the – when compared with 'true' AI – simple algorithms widely deployed in many different industries today can have a far-reaching impact on the forms of and conditions for competitive business conduct in these markets.[5] This fact in itself mandates competition law to scrutinize algorithmic implications and to intervene where they risk distorting competition. The interaction of algorithms and its collusive potential is (at present) one focal point of this mandate,[6] another example is big data-based market power.[7] It

[1] https://www.independent.co.uk/news/science/stephen-hawking-transcendence-looks-at-the-implications-of-artificial-intelligence-but-are-we-taking-9313474.html (all internet sources last accessed 12 October 2018).

[2] Cf. Margrethe Vestager's speech, Bundeskartellamt 18th Conference on Competition, 16 March 2017, https://ec.europa.eu/commission/commissioners/2014-2019/vestager/announcements/bundeskartellamt-18th-conference-competition-berlin-16-march-2017_en.

[3] An algorithm can be defined as a precise sequence of instructions to perform a task, *see* for instance https://dictionary.cambridge.org/dictionary/english/algorithm.

[4] The term AI was coined by John McCarthy in 1956 and now commonly refers to machines imitating human intelligence, *see* for the different definitions on AI Bernard Marr, *The Key Definitions Of Artificial Intelligence (AI) That Explain Its Importance*, https://www.forbes.com/sites/bernardmarr/2018/02/14/the-key-definitions-of-artificial-intelligence-ai-that-explain-its-importance/#3c01e9874f5d; machine learning, a subfield of AI, refers to algorithms that learn from data and experience to build intelligent machines; deep learning, a subfield of machine learning, is based on faster and more accurate learning, although no information on the decision-making process will be known (OECD (2017), *Algorithms and Collusion: Competition Policy in the Digital Age*, 9-11, www.oecd.org/competition/algorithms-collusion-competition-policy-in-the-digital-age.htm).

[5] OECD, *supra* n. 4, at 11-14.

[6] Cf. *infra* section 3.1.

[7] Cf. *infra* section 3.2.

seems not clear, though, that competition law has, in its present shape, the necessary rules and techniques to perform the task. Thus, it may be helpful to look at other areas of the law, which are more advanced in this respect, and to learn from their experience.

There is, however, yet another prong to the interaction of digitalization and competition law which forms part of a broader trend: In the EU at least, competition law enforcement has proven to be a tool of considerable efficiency.[8] It can, therefore, appear attractive to use this tool for resolving issues which do not belong to the core realm and goals of competition law – although they may be related to them. Outside the (direct) algorithmic context, the application of competition law to the licensing of intellectual property (IP) seems, in part, driven by this trend.[9] Within the context of algorithms, (consumer) data protection may become a prominent example.[10] As legal rules are, to a large extent, subordinate to the goals society wants to achieve with them, the employment of competition law to address issues beyond the mere protection of undistorted competition is not inherently flawed, especially where such issues are closely linked to an undistorted competitive process. It seems worthwhile, though, to ponder whether other areas of the law may, given their structure and resources, be in a better position to do the job.

Against this background, the present paper pursues a threefold, 'tool-box-oriented' task: Its second section assesses important examples of how other areas of the law deal with algorithm-based market activity.[11] The third section sketches three prototypical competitive concerns algorithms may evoke.[12] In the paper's fourth section, we ask whether competition law's present tool-box suffices to tackle these concerns, to which extent it may adopt tools used in other areas of the law, and whether, beyond mere adaptation, the development of new instruments seems necessary.[13] The final section summarizes and tries to sketch how our findings may induce a reflection on the allocation of algorithm-related tasks between different areas of the law.[14]

[8] This is illustrated by the prominent cases against big tech companies. Besides cases against Google (cf. *infra* section 3.2[a] and n. 145) and Facebook (on the German Bundeskartellamt's inquiry cf. *infra* section 3.3), the EU Commission is now also investigating against Amazon (https://www.ft.com/content/a8c78888-bc0f-11e8-8274-55b72926558f).
[9] Peter Picht, *Unwired Planet v. Huawei: A Seminal SEP/FRAND Decision from the UK*, (7) GRUR Int. 569, 576-577 (2017).
[10] Cf. *infra* section 3.3.
[11] Cf. *infra* section 2.
[12] Cf. *infra* section 3.
[13] Cf. *infra* section 4.
[14] Cf. *infra* section 5.

2. The legal tool box for algorithms outside competition law – examples and categories

2.1. Regulation of algorithmic trading in financial markets

With the implementation of algorithmic trading, financial markets were among the first to broadly and intensely deploy algorithms as a technical basis for economic market activity. Financial market regulation had to react and developed a comparatively detailed set of rules on algorithmic trading. As to the EU,[15] Germany pioneered with its 'Hochfrequenzhandelsgesetz'[16] and the EU followed suit, issuing the Directive 'on markets in financial instruments'[17] (MiFID II). Based to a large extent on the European Securities and Market Authority's ('ESMA')[18] Guidelines on 'Systems and Controls in an Automated Trading Environment for Trading Platforms, Investment Firms and Competent Authorities',[19] the Directive deals in meticulous detail with several aspects of algorithmic trading (AT) and high-frequency trading (HFT). Until 3 March 2019, the European Commission will present a report to the European Parliament and the Council on the impact of MiFID's AT/HTF requirements.[20] Its findings should be thoroughly considered when implementing similar tools in competition law.

According to MiFID II terminology, AT means the automatic determination of an order by a computer algorithm with minimal or no human intervention.[21] HFT is considered to be a subset of AT in which 'a trading system analyses data or signals from the market at high speed and then sends or updates large numbers of orders within a very short time period in response to that analysis'.[22] AT, and HFT in particular, can have positive effects on financial markets, for instance by improving order execution, increasing market liquidity as well as trading volume, narrowing bid and ask spreads, and reducing short

[15] Rules in other jurisdictions, such as Switzerland or the United States, are not examined in this paper.
[16] Hochfrequenzhandelsgesetz of 7 May 2013 – Bundesgesetzblatt 2013 Teil I Nr. 23, 14 May 2013, 1162-1166, http://dipbt.bundestag.de/extrakt/ba/WP17/479/47951.html.
[17] Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU.
[18] https://www.esma.europa.eu; *see* for Technical standards under Directive 2004/39/EC (MiFID I), Directive 2014/65/EU (MiFID II) and Regulation (EU) No 600/2014 (MiFIR): http://ec.europa.eu/finance/securities/docs/isd/mifid/its-rts-overview-table_en.pdf.
[19] Recital 63 MiFID II; *see* for the guidelines https://www.esma.europa.eu/sites/default/files/library/2015/11/esma_2012_122_en.pdf.
[20] Art. 90 para. 1 (c) MiFID II.
[21] Art. 4 para. 1 (39) and Recital 59 MiFID II.
[22] Recital 61 MiFID II; more precise definition in Art. 4 para. 1 (40) MiFID II.

term volatility.[23] But they can also pose specific risks, for example an increased likelihood for duplicate or erroneous orders, possible 'automatic' overreactions to market events, or information asymmetries resulting from an inequality of technical (viz. mainly: algorithmic) arms.[24] To fight these risks, MiFID II uses a combination of measures directed at firms engaging in algorithmic or high-frequency trading, at those providing electronic access, and at operators of trading venues.[25] In addition to MiFID II, the EU Market Abuse regulation (MAR)[26] prohibits some activities relating to algorithmic and high-frequency trading by qualifying them as market manipulation.[27]

2.1.[a] Investment firms

MiFID II sets up several duties for firms engaging in AT and HFT.[28] In particular,[29] they shall have in place:[30]

- 'effective systems and risk controls suitable to the business it operates to ensure that its trading systems are resilient and have sufficient capacity, are subject to appropriate trading thresholds and limits and prevent the sending of erroneous orders or the systems otherwise functioning in a way that may create or contribute to a disorderly market';
- 'effective systems and risk controls to ensure the trading systems cannot be used for any purpose that is contrary to' the MAR[31] 'or to the rules of a trading venue to which it is connected';
- 'effective business continuity arrangements to deal with any failure of its trading systems'.

[23] Recital 62 MiFID II; *see also* Megan Woodward, *The Need for Speed: Regulatory Approaches to High Frequency Trading in the United States and the European Union*, 50 Vand. J. Transnat'l L. 1359, 1368-1369 (2017).
[24] Recital 62 MiFID II.
[25] Recital 63 MiFID II.
[26] Regulation (EU) No 596/2014 of the European Parliament and of the Council of 16 April 2014 on market abuse (market abuse regulation) and repealing Directive 2003/6/EC of the European Parliament and of the Council and Commission Directives 2003/124/EC, 2003/125/EC and 2004/72/EC.
[27] Art. 12 para. 2 lit. c MAR.
[28] Since HFT is a subset of AT, specific rules on AT also apply to investment firms engaging in HFT (Danny Busch, *MiFID II: regulating high frequency trading, other forms of algorithmic trading and direct electronic market access*, 10(2) LFMR 72, 75 *in fine* (2016)).
[29] Besides, i.a., requiring authorisation (Art. 5 MiFID II).
[30] Art. 17 para. 1 MiFID II.
[31] Cf. *supra* n. 26.

To ensure that they meet these requirements, investment firms shall fully test and properly monitor their systems.[32] Regulatory Technical Standards 6 (RTS 6) set out the details of the organizational requirements for this testing and monitoring exercise.[33] The testing requirements include testing prior to deployment or update of the algorithms,[34] an appropriate allocation of responsibilities,[35] as well as a testing approach that secures the algorithm's conformance with the system of the trading venue or of the direct market access provider.[36] Some of the tests have to be undertaken in a sandbox-like testing environment.[37] An annual self-assessment and validation requirement[38] includes a stress testing of the algorithmic trading system.[39] The monitoring side includes the requirement to establish a 'kill functionality' resulting in the cancelation of some or all orders as an emergency measure.[40] As stated above, disruptive events must also be pre-emptively addressed by concluding business continuity agreements.[41] Furthermore, algorithmic trading activity ought to be monitored real-time,[42] and ESMA requests a surveillance of the systems of the investment firm for market manipulation.[43]

Several requirements touch on the investment firm's duty to document and store information:

– Investment firms engaging in algorithmic trading are required to notify this to the competent authorities of the trading venue and of its Member State.[44]

[32] Art. 17 para. 1 MiFID II.
[33] Commission Delegated Regulation (EU) 2017/589 of 19 July 2016 supplementing Directive 2014/65/EU of the European Parliament and of the Council with regard to regulatory technical standards specifying the organizational requirements of investment firms engaged in algorithmic trading, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32017R0589&from=EN.
[34] Art. 5 RTS 6.
[35] Art. 5 para. 3 RTS 6; cf. also Art. 1 and Recital 3 RTS 6: 'As a part of its overall governance framework and decision making framework, an investment firm should have a clear and formalised governance arrangement, including clear lines of accountability, effective procedures for the communication of information and a separation of tasks and responsibilities'.
[36] Art. 6 RTS 6.
[37] Art. 7 RTS 6: 'an environment that is separated from its production environment and that is used specifically for the testing and development of algorithmic trading systems and trading algorithms'. For sandboxing in financial markets *see also* the regulatory sandbox of the Financial Conduct Authority in the UK (https://www.fca.org.uk/publication/research/regulatory-sandbox.pdf and https://www.fca.org.uk/publication/research-and-data/regulatory-sandbox-lessons-learned-report.pdf).
[38] Art. 9 RTS 6.
[39] Art. 10 RTS 6.
[40] Art. 12 RTS 6.
[41] Art. 14 RTS 6.
[42] Art. 16 RTS 6.
[43] Art. 13 RTS 6.
[44] Art. 17 para. 2 subpara. 1 MiFID II.

- The latter may require the investment firm to provide (regularly or ad-hoc) 'a description of the nature of its algorithmic trading strategies, details of the trading parameters or limits to which the system is subject, the key compliance and risk controls that it has in place to ensure the conditions laid down in paragraph 1 are satisfied and details of the testing of its systems. The competent authority of the home Member State of the investment firm may, at any time, request further information from an investment firm about its algorithmic trading and the systems used for that trading'.[45]
- In any case, such information has to be passed on at the request of competent authorities of a trading venue at which the investment firm undertakes algorithmic trading.[46]
- All this information has to be documented.[47]
- Moreover, investment firms engaging in HFT[48] have to keep accurate and time sequenced records of all orders and make them available to the competent authority upon request.[49]

Mere mention be made of a set of provisions applying to market making strategies of AT investment firms[50] and of duties related to an investment firm's granting traders direct electronic access to a trading venue.[51] These rules address algorithmic trading activity but they are keyed very specifically to the financial sector and, hence, of limited transfer value.

2.1[b] Trading Venues

In general, trading venues[52] shall establish resilient and tested trading systems and shall be able to deal with large order volumes and markets under stress.[53] Trading venues to which AT and HFT traders are connected have to meet additional requirements laid down in

[45] Art. 17 para. 2 subpara. 2 MiFID II.
[46] Art. 17 para. 2 subpara. 3 MiFID II.
[47] Art. 17 para. 2 subpara. 4 MiFID II.
[48] If they only engage in AT, they must also keep their transaction data due to the general provisions of Art. 25 MiFIR (Regulation (EU) No 600/2014 of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Regulation (EU) No 648/2012) and Art. 16 para. 6 MiFID II.
[49] Art. 17 para. 2 subpara. 5 MiFID II.
[50] Art. 17 para. 3 MiFID II.
[51] Cf. Art. 4 para. 1 (41), Art. 17 para. 5 MiFID II; cf. in detail Busch, *supra* n. 28, at 75 and 77-78.
[52] Consisting of regulated markets, multilateral trading facilities (MTFs) and organized trading facilities (OTFs), cf. Art. 4 para. 1 (24) MiFID II.
[53] Art. 48 para. 1 MiFID II for regulated markets, in conjunction with Art. 18 para. 5 MiFID II for MTFs and OTFs.

Regulatory Technical Standards 7 (RTS 7).[54] These include monitoring obligations regarding the adaptation and robustness of their AT systems, including real-time monitoring of their performance and capacity as well as of member's orders,[55] and a periodical review of the performance and capacity of the algorithmic trading systems as a whole.[56] Furthermore, trading venues shall have in place a kill functionality to be able to cancel certain orders,[57] carry out a due diligence regarding their members,[58] and test their trading systems.[59] As a kind of compensation, trading venues are permitted to charge higher fees for AT and HFT.[60]

Similar to investment firms, trading venues are required to 'have in place effective systems, procedures and arrangements, including requiring members or participants to carry out appropriate testing of algorithms and providing environments to facilitate such testing, to ensure that algorithmic trading systems cannot create or contribute to disorderly trading conditions on the market and to manage any disorderly trading conditions which do arise from such algorithmic trading systems'.[61] These tests include a requirement for the members to conduct conformance testing in the testing environment of the trading venue[62] so as to avoid disorderly trading conditions.[63] Trading venue members must flag and trading venues must be able to identify algorithmic orders, as well as the used algorithms and their initiator, and the venues must provide this information to competent authorities upon request.[64]

2.2. General Data Protection Regulation

Data protection law is another area that already has in place certain elements of a legal framework for algorithmic (market) activity. This is true, in particular, for the EU's General Data Protection Regulation

[54] Busch, *supra* n. 28, at 78; Art. 1 para. 1 of Commission Delegated Regulation (EU) 2017/584 of 14 July 2016 supplementing Directive 2014/65/EU of the European Parliament and of the Council with regard to regulatory technical standards specifying organizational requirements of trading venues, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32017R0584&from=EN.
[55] Art. 12 RTS 7.
[56] Art. 14 RTS 7.
[57] Art. 18 para. 2 (c) RTS 7.
[58] Art. 7 RTS 7.
[59] Art. 8 RTS 7.
[60] Art. 48 para. 9 subpara. 3 (regulated markets) and Art. 18 para. 5 (MTFs and OTFs) MiFID II.
[61] Art. 48 para. 6 MiFID II.
[62] Art. 9 RTS 7.
[63] Art. 10 RTS 7.
[64] Art. 48 para. 10 MiFID II.

(GDPR),[65] but also for the ePrivacy Regulation probably to be enacted sometime in 2019, forming a *lex specialis* to the GDPR, and applying i.a. to machine-to-machine communication.[66]

The GDPR includes,[67] in its Art. 22 para. 1, a provision that gives the data subject[68] 'the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her'. Art. 4(4) GDPR defines profiling as 'any form of automated processing[69] of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person'. As an addition to Art. 22, recital 71 formulates some requirements for profiling algorithms, which 'should use appropriate mathematical or statistical procedures' to minimize the risk of errors and prevent discriminatory effects.[70] A decision based solely on automated processing is permissible, if it 'is necessary for entering into, or performance of, a contract'[71] or if it the data subject has given his explicit consent.[72] In such cases, however, the 'data controller' has a duty to implement suitable procedures, with a minimum standard of protection consisting of a right of the data subject to obtain human

[65] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). On the Regulation in general, see Tobias Lettl, *Die Datenschutz-Grundverordnung (DSGVO)*, (25) WM 1149 (2018); Indra Spiecker gen. Döhmann, Vagelis Papakonstantinou, Gerrit Hornung & Paul de Hert, *European General Data Protection Regulation*, C.H.Beck forthcoming.

[66] Cf. Recital 12 of the proposed Directive (https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-privacy-and-electronic-communications):
'Connected devices and machines increasingly communicate with each other by using electronic communications networks (Internet of Things). The transmission of machine-to-machine communications involves the conveyance of signals over a network and, hence, usually constitutes an electronic communications service. In order to ensure full protection of the rights to privacy and confidentiality of communications, and to promote a trusted and secure Internet of Things in the digital single market, it is necessary to clarify that this Regulation should apply also to the machine-to-machine communications whenever these are related to users. Therefore, the principle of confidentiality enshrined in this Regulation should also apply to the transmission of machine-to-machine communications. Specific safeguards could also be adopted under sectorial legislation, as for instance Directive 2014/53/EU.'

[67] The preceding Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data already contained a similar provision in Art. 15.

[68] *See* Art. 4(1) GDPR.

[69] And thus encompassing algorithms, cf. Mario Martini, *Datenschutz-Grundverordnung, Bundesdatenschutzgesetz: DS-GVO BDSG*, Art. 22 para. 21 (Boris P. Paal & Daniel A. Pauly, 2nd ed., C.H.Beck 2018).

[70] Martini, *supra* n. 69, at Art. 22 para. 36.

[71] Art. 22 para. 2 lit. a GDPR.

[72] Art. 22 para. 2 lit. b GDPR.

intervention and to express his or her point of view if he/she wishes to contest the decision.[73] The definition of 'suitable measures' does, however, not seem to go as far as to require the algorithm to be disclosed.[74] Art. 13 para. 2 lit. f[75] GDPR stipulates that the use of automated decision making shall be communicated to the data subject, including 'meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.' It is disputed whether Art. 13 constitutes a duty to disclose the algorithm itself, with the leading opinion answering this question in the negative because this would result in a forced disclosure of trade secrets.[76] Art. 22 GDPR tries to mitigate the risks associated with automated decision-making based on algorithms.[77] While the provision's implications appear limited[78] due to its narrow focus on automation without human interference, it is at least an attempt at protecting citizens from uncontrolled algorithmic decision-making.[79]

Under Art. 20 GDPR and its corresponding Guidelines[80] and Recitals, the 'data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided'. This 'data portability right' applies to all sectors of the economy and conveys not necessarily ownership of but certainly a

[73] Art. 22 para. 3 GDPR.

[74] Martini, *supra* n. 69, at Art. 22 para. 36; Benedikt Buchner, *Datenschutz-Grundverordnung, Bundesdatenschutzgesetz: DS-GVO/BDSG*, Art. 22 para. 35 (Jürgen Kühling & Benedikt Buchner, 2nd ed., C.H.Beck 2018); Sandra Wachter, Brent Mittelstadt & Luciano Floridi, *Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation*, 7(2) IDPL 76, 94 (2017).

[75] Cf. also Art. 14 para. 2 lit. g and Art. 15 para. lit. h GDPR.

[76] Boris Paal & Moritz Hennemann, *Datenschutz-Grundverordnung, Bundesdatenschutzgesetz: DS-GVO BDSG*, Art. 13 para. 31 (Boris P. Paal & Daniel A. Pauly, 2nd ed., C.H.Beck 2018); Holger Greve, *Europäische Datenschutzgrundverordnung*, Art. 12 para. 7 (Gernot Sydow, 2nd ed., Nomos 2018); Marcus Helfrich, *id*., Art. 22 para. 79 (regarding Art. 15 para. 1 lit. h GDPR); Matthias Bäcker, *Datenschutz-Grundverordnung, Bundesdatenschutzgesetz: DS-GVO/BDSG*, Art. 13 para. 54 (Jürgen Kühling & Benedikt Buchner, 2nd ed., C.H.Beck 2018); Wachter, Mittelstadt & Floridi, *supra* n. 74, at 89-90.

[77] Martini, *supra* n. 69, Art. 22 para. 8.

[78] Ulrich Dammann, *Erfolge und Defizite der EU-Datenschutzgrundverordnung, Erwarteter Fortschritt, Schwächen und überraschende Innovationen*, (7) ZD 307, 312-313 (2016).

[79] OECD, *supra* n. 4, at 49; Martini, *supra* n. 69, at Art. 22 para. 46.

[80] The so-called 'Article 29 Data Protection Working Party', a body composed of representatives of the Member States' data protection authorities, of the European Data Protection Supervisor, and of the European Commission, issued Guidelines on Art. 20 GDPR, *see* Article 29 Data Protection Working Party, *Guidelines on the right to data portability*, 5 April 2017, 16/EN WP 242 rev.01, http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611233.

far-reaching right to control and duplicate the use of the pertinent personal data.[81] Its potential implications are manifold and far-reaching. Among them are the questions of how to define 'personal data … provided to a controller', the only type of data subject to the portability right;[82] of how a data subject may use its portability right as a basis for transacting over its data, e.g. by assigning to third parties a claim to access the data; of whether the data subject must wait until the controller has collected and assembled the data or whether Art. 20 GDPR implies a right to directly collect data regardless of the collector's business secrets being affected by such an act; of whether portability creates an ownership-like control over ported data; or of how to balance, mainly in the application of Art. 20 para. 4 GDPR,[83] the portability right with intellectual property rights extending to the respective data.[84]

Other provisions of the GDPR may be relevant for algorithms as well. Self-learning algorithms (and their use), for instance, may qualify as a form of 'new technologies' under Art. 35 para. 1 GDPR, thus requiring a prior data protection impact assessment of the envisaged processing operations.[85] The GDPR also stipulates 'data protection by design and by default'.[86] This refers to the requirements of implementing, already in the design phase, appropriate technical and organisational measures to protect the data subject's rights,[87] and of processing, by default, only data necessary for the respective, specific purpose.[88]

[81] Inge Graef, Martin Husovec & Nadezhda Purtova, *Data Portability and Data Control, Lessons for an Emerging Concept in EU Law*, (22) Tilburg Law School Legal Studies Research Paper Series 1, 5, 7, 19 (2017), https://ssrn.com/abstract=3071875.

[82] On this, *see* Colette Cuijpers, Nadezhda Purtova & Eleni Kosta, *Data Protection Reform and the Internet: the Draft Data Protection Regulation*, 558 (Andrej Savin & Jan Trzaskowski, Research Handbook on EU Internet Law, Edward Elgar 2014); Graef, Husovec & Purtova, *supra* n. 81, at 9-10.

[83] Art. 20 para. 4 GDPR states that '[t]he right referred to in paragraph 1 shall not adversely affect the rights and freedoms of others' and provides, thereby, the basis for a balancing of the data portability right against other affected rights, such as the right to freedom of expression and information (Art. 11 Charter of Fundamental Rights of the European Union) or intellectual property rights relating to the data to-be-ported; *see* Hans-Georg Kamann & Martin Braun, *Datenschutz-Grundverordnung: DS-GVO*, Art. 20 para 33-37 (Eugen Ehmann & Martin Selmayr, 2nd ed., C.H.Beck 2018).

[84] Article 29 Data Protection Working Party, *supra* n. 80, at 12; Graef, Husovec & Purtova, *supra* n. 81, at 10-13.

[85] Martini, *supra* n. 69, at Art. 35 para. 18 and 77.

[86] Art. 25 and Recital 78 GDPR.

[87] Joachim Schrey, *New European General Data Protection Regulation: A Practicioner's Guide*, para. 530 (Daniel Rücker & Tobias Kugler, C.H.Beck 2018).

[88] Schrey, *supra* n. 87, at para. 533.

2.3. Categorizing regulatory tools

The numerous, detailed provisions dealing with algorithms, and the AI they may drive, reflect, beyond context-related specificities, several basic principles that are likely to be valid across various areas of the law. In 2017, the Association for Computing Machinery (ACM) published a statement on algorithmic transparency and accountability[89] that distinguishes seven fundamental principles, namely awareness,[90] access and redress,[91] accountability,[92] explanation,[93] data provenance,[94] auditability[95] and validation and testing.[96] Similarly, an analysis of the policy instruments under consideration by the House of Commons Science and Technology Committee on 'algorithms in decision-making' by Leighton Andrews led to the following classification:[97] Technical,[98] governance,[99]

[89] Statement on Algorithmic Transparency and Accountability, by ACM U.S. Public Policy Council and ACM Europe Policy Committee, updated 25 May 2017, https://www.acm.org/binaries/content/assets/public-policy/2017_joint_statement_algorithms.pdf.

[90] 'Owners, designers, builders, users, and other stakeholders of analytic systems should be aware of the possible biases involved in their design, implementation, and use and the potential harm that biases can cause to individuals and society.'

[91] 'Regulators should encourage the adoption of mechanisms that enable questioning and redress for individuals and groups that are adversely affected by algorithmically informed decisions.'

[92] 'Institutions should be held responsible for decisions made by the algorithms that they use, even if it is not feasible to explain in detail how the algorithms produce their results.'

[93] 'Systems and institutions that use algorithmic decision-making are encouraged to produce explanations regarding both the procedures followed by the algorithm and the specific decisions that are made. This is particularly important in public policy contexts.'

[94] 'A description of the way in which the training data was collected should be maintained by the builders of the algorithms, accompanied by an exploration of the potential biases induced by the human or algorithmic data-gathering process. Public scrutiny of the data provides maximum opportunity for corrections. However, concerns over privacy, protecting trade secrets, or revelation of analytics that might allow malicious actors to game the system can justify restricting access to qualified and authorized individuals.'

[95] 'Models, algorithms, data, and decisions should be recorded so that they can be audited in cases where harm is suspected.'

[96] 'Institutions should use rigorous methods to validate their models and document those methods and results. In particular, they should routinely perform tests to assess and determine whether the model generates discriminatory harm. Institutions are encouraged to make the results of such tests public.'

[97] Leighton Andrews, *Algorithms, governance and regulation: beyond 'the necessary hashtags'*, (85) LSE Discussion Paper 7, 18 (2017), https://www.kcl.ac.uk/law/research/centres/telos/assets/DP85-Algorithmic-Regulation-Sep-2017.pdf.

[98] Transparency, accountability and explicability; best practice; training data of algorithm to be prescribed; distinctions between basic and machine learning algorithms; further research on technical mechanisms to interrogate 'black box'.

[99] Internal compliance teams; GDPR compliance certification; public sector algorithms to be analyzed in line with MacPherson review of government

regulation,[100] legislative[101] and institutional,[102] while noting the absence of any fiscal instruments.

Trying to merge these principles and classifications, the examples described above, and a number of further pertinent provisions into a graticule of regulatory tools, one may arrive at the following categorization:

Transparency

- Duty to inform (Art. 13 Abs. 2 lit. f GDPR), to describe (Art. 17 para. 2 subpara 2 MiFID II), to notify (Art. 17 para. 2 subpara. 1 MiFID II) and to flag (Art. 48 para. 10 MiFID II)
- Claims to information (Art. 15 Abs. 1 lit. h GDPR, Art. 17 para. 2 subpara. 3 and 5 MiFID II)
- Access and transfer rights (Art. 15 para. 3 and Art. 20 GDPR)
- Duty to document (Art. 16 para. 6 MiFID II) and to keep reports (Art. 17 para. 2 subpara. 4 MiFID II)

Prevention/deterrence

- Prohibition (Art. 22 para. 1 GDPR)
- Authorization (Art. 5 MiFID II)
- Impact assessment (Art. 35 para. 1 GDPR)

Intervention

- Kill functionality (Art. 12 RTS 6, Art. 18 para. 2 (c) RTS 7)

modelling; develop professional standards for data science; support role of partnership for AI.

[100] Sectoral statutory oversight body (e.g. police); new scrutiny and oversight duties on existing regulators; requirements not to design algorithms which challenge protected characteristics under HR law; requirement for EIAs or HIRIAs for algorithms; GDPR as basis of regulation; medical algorithms to be subjected to MHRA; CMA to investigate pricing algorithms.

[101] Legally mandated 'right to explanation' of automated decisions to supplement GDPR; Humanly interpretable decision-making methods in mandated risky sectors; categorization of risky and non-risky sectors/mechanisms; right to challenge by those affected; mandation of certification mechanisms to ensure fair, open and non-discriminatory practices prior to deployment of algorithms.

[102] Algorithmic or machine learning or data ethics oversight institution with proper resourcing or/and capacity building for existing regulators; investment in public R&D on algorithms; technical oversight and template design; analyses algorithmic experience from creditscoring industry as potential for best practice in accountability.

– Business continuity agreements (Art. 14 RTS 6)

Standard setting

– Effective systems and risk control (Art. 17 para. 1 MiFID II)
– Requirements for algorithms (Recital 71 GDPR)
– (Data) protection by default and design (Art. 25 GDPR)
– Due diligence (Art. 14 RTS 7)

Liability – and its steering effect

– Disincentive fees (Art. 48 para. 9 subpara. 3 MiFID II)
– Allocation of responsibility (Art. 5 para 3 RTS 6)

Testing and monitoring (Art. 17 Para. 1 MiFID II)

– Ex-ante (Art. 5 RTS 6) and/or sandboxing (Art. 7 RTS 6)
– Real-time (Art. 16 RTS 6, Art. 13 RTS 6)
– Ex-post[103]/periodic (Art. 9 RTS 6, Art. 10 RTS 6, Art. 14 RTS 7)

Enforcement[104]

– Agency enforcement
– Right of associations to initiate proceedings
– Mediation/arbitration bodies
– Specific unfair competition warning letters
– Competence to order specific measures (cf. testing and transparency)
– Specific burden of proof

Broader regulatory framework[105]

– (Ethical) guidelines[106]

[103] Cf. also *Autocomplete*, Az. VI ZR 269/12 (BGH 14 May 2013).
[104] Cf. also *infra* section 4 and 5.
[105] Cf. also *infra* section 4 and 5.

- Self-regulation
- Certification of algorithms
- Artificial Intelligence Development Act[107]
- International Artificial Intelligence Organization[108]

3. Prominent algorithmic issues in the field of competition law

We cannot, today, foresee all the facets of AI and algorithmic market activity which may come under competition law scrutiny and this paper cannot even attempt to detail the gamut of constellations whose relevance we already perceive. We therefore limit this section to three types of cases that are both much discussed at present and potentially prototypical for the intersection of algorithms and competition law.

3.1. Algo collusion[109]

The competitive process risks suffering harm when competitors make arrangements regarding their market activity. Such arrangements are usually called 'collusion' if they serve to raise the coordinating parties' profits above the non-cooperative equilibrium.[110] 'Explicit collusion' rests on an agreement or some other form of concertation between the involved market players, while 'tacit collusion',[111] oftentimes leading to 'parallel behaviour', requires no such concertation and can, in particular, result from market players monitoring and reacting to each other's independent business decisions.[112] Both types of collusion are economically undesirable as they tend to result in supra-competitive prices, lower output, deadweight losses, and, ultimately, a reduction in (consumer)

[106] *See*, for instance, the EU's endeavor to ensure the transparency of algorithms, which will be addressed in the AI ethics guidelines to be released by the end of the year http://europa.eu/rapid/press-release_MEMO-18-3363_en.htm.
[107] Matthew U. Scherer, *Regulating Artificial Intelligence Systems: Risks, Challenges, Competencies, and Strategies*, 29(2) Harv. J.L. & Tech. 354 (2016).
[108] Olivia J. Erdélyi & Judy Goldsmith, *Regulating Artificial Intelligence, Proposal for a Global Solution*, http://www.aies-conference.com/2018/contents/papers/main/AIES_2018_paper_13.pdf.
[109] This section is based to a large extend on Peter Georg Picht & Benedikt Freund, *Competition (law) in the era of Algorithms*, 39(9) E.C.L.R. 403 (2018).
[110] OECD, *supra* n. 4, at 19; cf. also Hal R. Varian, *Intermediate Microeconomics – A modern Approach*, 531-532 (9th ed., W. W. Norton & Company 2014).
[111] Cf. Richard A. Posner, *Antitrust Law*, 52-53 (2nd ed., University of Chicago Press 2001).
[112] Michael K. Vaska, *Conscious Parallelism and Price-fixing: Defining the Boundary*, 52(2) U Chi L Rev 508, 509, 519-520 (1985); cf. also Picht & Freund, *supra* n. 109, at 404.

welfare.[113] Nonetheless, most competition law regimes prohibit – at present – only explicit collusion while tolerating tacit collusion and parallel behaviour, not least because banning tacit collusion may inhibit market players from intelligently adapting their business strategy to their competitors' prices or other market conditions – after all a key component of competitive behaviour.[114]

Algorithms can, in various ways, be tools for establishing explicit collusion.[115] The use of identical pricing algorithms by competitors, for instance, is – arguably – not unlawful as such[116] but it can help competitors to unlawfully align their prices as part of a joint and consented strategy reducing competitive pressure.[117] Instead of

[113] OECD, *supra* n. 4, at 19-20; Alison Jones & Brenda Sufrin, *EU Competition Law, Text, Cases and Materials*, 650 (6th ed., Oxford University Press 2016).

[114] For the EU: *Ahlström Osakeyhtiö and others v. Commission*, C-89/85, para. 71 (ECJ 31 March 1993); *Suiker Unie and Others v Commission, C-40/73*, para. 174 (ECJ 16 December 1975); cf. also Jones & Sufrin, *supra*. n. 113, at 694-698; for the US: *In re: Text Messaging Antitrust Litigation*, No. 14-2301, 10-11 (7th Cir. 9 April 2015).

[115] Cf. Ariel Ezrachi & Maurice E. Stucke, *Artificial Intelligence & Collusion: When Computers Inhibit Competition*, U. Ill. L. Rev. 1775, 1784-1787 (2017).

[116] *See* Advocate General Szpunar's remark in a footnote in the Uber case: 'the use by competitors of the same algorithm to calculate the price is not in itself unlawful, but might give rise to hub-and-spoke conspiracy concerns when the power of the platform increases' (*Asociación Profesional Elite Taxi*, C‑434/15, fn. 23 (Opinion of Advocate General Szpunar 11 May 2017)).

[117] *United States v. David Topkins*, Plea Agreement, No. CR 15 201 WHO (N.D. Cal. 30 April 2015), https://www.justice.gov/atr/case-document/file/628891/download; *United States v. David Topkins*, No. CR 15 201 WHO (N.D. Cal. 6 April 2015), https://www.justice.gov/atr/case-document/file/513586/download; cf. also Salil K. Mehra, *US v. Topkins: Can Price Fixing be Based on Algorithms?*, 7(7) JIPLP 470 (2016); Virgílio Pereira, *Algorithm-driven Collusion: Pouring old wine into new Bottles or new wine into Fresh Wineskins?*, 39(5) ECLR 212, 214-215 (2018); Jill Priluck, *When Bots Collude*, https://www.newyorker.com/business/currency/when-bots-collude; according to the Commission's report on the E-commerce Sector Inquiry 67 % of the 53 % of respondents tracking competitor's prices do so by automated systems and 78 % of those 67 % adjust their prices (European Commission, Preliminary Report on the E-commerce Sector Inquiry, 15 September 2016, SWD(2016) 312, 56, http://ec.europa.eu/competition/antitrust/sector_inquiry_preliminary_report_en.pdf); for an empirical analysis of algorithmic pricing on Amazon Marketplace *see* Le Chen, Alan Mislove & Christo Wilson, *An Empirical Analysis of Algorithmic Pricing on Amazon Marketplace*, https://mislove.org/publications/Amazon-WWW.pdf; cf. also the algorithmic resale price maintenance case involving Asus, Denon & Marantz, Philips and Pioneer, http://europa.eu/rapid/press-release_IP-18-4601_en.htm; Michal Gal sees possible unlawful conduct where competitors (1) start consciously using similar algorithms, despite better algorithms being available, (2) feed the same or similar training data to the learning algorithm, despite better training data being available and despite the awareness of the possibility of similar pricing results, or (3) make the algorithm transparent to competitors without any procompetitive justification (Caron Beaton-Wells, *Competition Lore Podcast, Competition and algorithms – friend or foe?*, episode of 19 September 2018, https://overcast.fm/+N2zZD5F3Q/55:13).

such a decentralized strategy, competitors may jointly implement[118] a 'hub and spoke' cartel, for instance[119] by delegating the setting of prices (and potentially other conditions) to a central, algorithmic agent.[120] The coordination necessary to establish the hub and spoke structure typically requires some form of explicit collusion. The 'signalling' strategy – another option – employs algorithms to exchange concealed information about (planned) market behaviour by sending, as it were, a Morse code, for instance in the form of patterned, short-term price changes which are being planned, executed and registered by algorithms.[121]

Whatever the strategy, explicit collusion remains illegal, regardless of whether it is being implemented by traditional, analogue techniques or by cutting-edge algorithms.[122] The challenges algorithmic explicit collusion presents consist, hence, not in deciding whether such conduct should be banned but rather in assessing its likelihood, detecting it in specific cases, and assigning appropriate liability.[123] Compared to more old-fashioned scenarios, several factors can complicate the uncovering of algorithmic collusion. For instance, algorithms can run their direct interaction at much higher speed than coordination involving humans (more directly)[124],[125] they can cloak it – in certain respects[126] – in patterns more complex than those of

[118] Hub and spoke settings are more likely to occur as the result of explicit collusion, although they may also result from implicit collusion.

[119] For further variants and details, *see* Ezrachi & Stucke, *supra* n. 115, at 1787-1788.

[120] *Meyer v. Kalanick*, No. 15 Civ. 9796, Opinion and Order (S.D.N.Y. 31 March 2016); *Eturas and Others*, C-74/14 (ECJ 21 January 2016); *see also* Andreas Heinemann & Aleksandra Gebicka, *Can Computers Form Cartels? About the Need for European Institutions to Revise the Concertation Doctrine in the Information Age*, 7(7) JECLAP 431 (2016).

[121] OECD, *supra* n. 4, at 29-30.

[122] Monopolkommission, XXII. Hauptgutachten: Wettbewerb 2018, para. 201, https://www.monopolkommission.de/images/HG22/HGXXII_Gesamt.pdf; cf. also EU Commission in its submission to the OECD: 'if pricing practices are illegal when implemented offline, there is a strong chance that they will be illegal as well when implemented online' (Directorate for Financial and Enterprise Affairs Competition Committee, *Algorithms and Collusion – Note from the European Union*, 14 June 2017, 9, https://one.oecd.org/document/DAF/COMP/WD(2017)12/en/pdf).

[123] Cf. Monopolkommission, Hauptgutachten 2018, *supra* n. 122, at para. 215, according to which algorithms represent the prior will of the user but a shift in liability may have to be considered regarding self-learning algorithms.

[124] Humans can be involved in algorithmic-collusion as well, of course, but more indirectly, as coders, implementers, beneficiaries, etc., not as those directly exercising the coordination.

[125] OECD, *supra* n. 4, at 22 with reference to the Autorité de la Concurrence, Bundeskartellamt, Competition Law and Data, 14-15, https://www.bundeskartellamt.de/SharedDocs/Publikation/DE/Berichte/Big%20Data%20Papier.pdf?__blob=publicationFile&v=2.

[126] Algorithms may be much better in devising and deciphering math patterns, but they may be much weaker in decoding the non-verbal and non-mathematical

human communication, and they are less (if at all) likely to succumb to weaknesses – fatigue, emotions (fear, anger, regret), irrationality – humans often show in their communicative interaction.[127]

Where competition law enforcers manage, nonetheless, to discover algorithmic collusion that violates the law, they must decide on the liability of and on sanctions for the humans having built, coded, implemented or profited from the colluding algorithm. This can pose questions of justice and effective liability design which we will assess in greater detail below.[128] Suffice it here to say that the degree of complexity and independence with which the algorithm operates ought probably to matter in this respect. This is because humans – the ultimate addressees of liability – exercise much more direct control over 'simple' algorithms that merely execute patterns initially coded into them[129] than over so-called 'deep learning' algorithms[130] which are able to make decisions based on their own artificial neural network, i.e. to a large extent independently of pre-set rules and parameters.

The use of truly deep-learning algorithms as part of companies' business models is purportedly rather limited at present.[131] Such algorithms are key drivers of AI, though, and very likely to spread widely in the years to come. This invests the third challenge mentioned above, viz. the assessment of and appropriate reaction to the likelihood of algorithmic collusion, with great importance. Since the illegality of explicit collusion is well established, an increased likelihood of this type of conduct due to the spread of algorithmic market activity mainly means that competition law enforcement ought to allot additional and appropriate resources to the field.[132]

Tacit collusion requires a more fundamental reflection: Besides other reasons,[133] competition law has – so far and except for cases of joint market dominance – tolerated[134] the detrimental economic effects of tacit collusion because conventional wisdom has it that this type of conduct requires rather specific conditions to succeed. In a nutshell, these conditions are (1) an oligopolistic market structure,[135] (2)

communication (a look, a wink of the eyes, a handshake, an ambiguous expression) with which humans are able to convey complex, multi-facetted messages.

[127] Ezrachi & Stucke, *supra* n. 115, at 1792-1793.

[128] Cf. *infra* section 4 and 5.

[129] Cf. Ezrachi & Stucke, *supra* n. 115, at 1787.

[130] Cf. OECD, *supra* n. 4, at 32.

[131] Cf. OECD, *supra* n. 4, at 12, for applications of deep learning.

[132] Cf. *infra* section 4 and 5.

[133] Cf. *supra* section 3.1.

[134] Joint market dominance only partially covers tacit collusion, cf. Monopolkommission, Hauptgutachten 2018, *supra* n. 122, at para. 217-224.

[135] Jan Potters & Sigrid Suetens, *Oligopoly Experiments in the Current Millennium*, 27(3) J. Econ. Surv. 439, 448 (2013).

homogeneity of goods and services in the market,[136] (3) market transparency,[137] and (4) high barriers for market entry.[138] Since these conditions appear(ed) to be present in a few markets only, the economic harm from tacit collusion seemed limited as well.[139] If (deep-learning) algorithms were to make tacit collusion less dependent on its traditional preconditions and, overall, more likely,[140] competition law's present approach towards tacit collusion may have to be reconsidered.[141] Algorithms may have such an effect, *inter alia* because they tend to increase transaction intensity,[142] thereby generating more data points with which to establish and control collusive equilibria, because their ability to analyse (big) data helps to understand competitors' conduct,[143] and because they are less prone

[136] Marc Ivaldi, Bruno Jullien, Patrick Rey, Paul Seabright & Jean Tirole, *The Economics of Tacit Collusion, Final Report for DG Competition*, 47, 66 (2013), http://ec.europa.eu/competition/mergers/studies_reports/the_economics_of_tacit_collusion_en.pdf.

[137] *See* Christian Schultz, *Transparency on the Consumer Side and Tacit Collusion*, 49(2) Eur. Econ. Rev 279, 280 (2003).

[138] OECD, *supra* n. 4, at 20-21; Michal S. Gal, *Algorithmic-Facilitated Coordination: Market and Legal Solutions*, 2 Antitrust Chronicle, 22-23 (2017), https://www.competitionpolicyinternational.com/wp-content/uploads/2017/05/AC_May.pdf.

[139] Salil K. Mehra, *Antitrust and the Robo-Seller: Competition in the Time of Algorithms*, 100 Minn. L. Rev. 1323, 1328 (2016); Rolf H. Weber, *Disruptive Technologies and Competition Law*, ch. 4.2.1 (Klaus Mathis, New Developments in Competition Law and Economics, Springer forthcoming); *see also* Autorité de la Concurrence, Bundeskartellamt, Competition Law and Data, *supra* n. 125, at 14-15.

[140] On (o)the(r) characteristics that make tacit collusion more likely *see* Competition and Markets Authority, Pricing Algorithms, Economic Working Paper on the use of Algorithms to Facilitate Collusion and Persoanlised Pricing, 8 October 2018, para. 12-15, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/746353/Algorithms_econ_report.pdf; Schwalbe argues that algorithmic collusion is more difficult to achieve than legal scholars assume, *see* Ulrich Schwalbe, *Algorithms, Machine Learning, and Collusion*, 2-3 for an overview, https://ssrn.com/abstract=323263; on this category of autonomous machines, cf. also Ezrachi & Stucke, *supra* n. 115, at 1795-1796.

[141] '[I]nstances of coordination through algorithms are likely to become more commonplace in our digital world. This also implies that one of the considerations underlying the rule which treats conscious parallelism as legal – that it can take place only in a limited number of highly concentrated markets and therefore is likely to create minor economic effects – no longer holds' (Michal Gal, *Algorithms as Illegal Agreements*, Berkeley Tech. L.J. 44 (forthcoming), https://ssrn.com/abstract=3171977); Picht & Freund, *supra* n. 109, at 405.

[142] Competition and Markets Authority, *supra* n. 140, at para. 5.27-5.28 and 8.3, also listing other risk factors related to algorithmic pricing possibly leading to coordination at para. 8.4-8.7.

[143] This feature may, for instance, play out in 'predictable agent' cases, that is, settings, in which competitors unilaterally use algorithmic tools that help to establish conscious parallelism by generating predictable outcomes and predicting each other's results, *see* Ezrachi & Stucke, *supra* n. 115, at 1789-1791.

than humans to biases and errors which may destabilize established collusion.[144]

3.2. Big data + algorithms = market dominance (and abuse)?

Cases relating to the use of algorithms by dominant market players are slowly moving into the antitrust spotlight. Two prominent examples are the EU Commission's Google Shopping and the German Bundeskartellamt's Lufthansa case.

3.2[a] Google Search (Shopping)

In one prong of Google's confrontation with competition agencies,[145] the EU Commission had to assess whether Google was abusing its dominance[146] on the search engine market and held the company did so by demoting rival comparison shopping services in its search results whilst prominently placing its own ('Google Shopping')[147].[148] The demotion was attributed to several criteria in Google's search algorithm and the fact that Google Shopping itself was not subject to the workings of the algorithm, resulting in significant gain in traffic for Google Shopping and losses for its competitors.[149] The decision raises several interesting questions, i.a. whether the EU Commission should have assumed a two-sided market,[150] how to categorize

[144] Cf. in detail Picht & Freund, *supra* n. 109, at 405.
[145] Among the other prongs are Google Android (http://ec.europa.eu/competition/elojade/isef/case_details.cfm?proc_code=1_40099) and Google AdSense (http://ec.europa.eu/competition/elojade/isef/case_details.cfm?proc_code=1_40411).
[146] The EU Commission found Google dominant in general internet search markets in all 31 countries of the European Economic Area (EEA) since 2008 (except in the Czech Republic since 2011) and abusing its dominance in all 13 EEA countries in which it offered Google shopping.
[147] It was initially called 'Froogle', later 'Google Product Search' and now 'Google Shopping'.
[148] Case AT.39740, *Google Search (Shopping)*, decision of 27 June 2017, http://ec.europa.eu/competition/antitrust/cases/dec_docs/39740/39740_14996_3.pdf.
[149] Cf. Commission press release IP/17/1784, http://europa.eu/rapid/press-release_IP-17-1784_en.htm.
[150] Rupprecht Podszun, *Der grosse Donner – hat sich Alphabet vergoogelt?*, https://www.d-kart.de/der-grosse-donner-hat-sich-alphabet-vergoogelt; on two- and multi-sided markets: Thomas Hoppner, *Defining Markets for Multi-Sided Platforms: The Case of Search Engines*, 38(3) WC 349 (2015); Stefan Holzweber, *Market Definition for Multi-Sided Platforms: A Legal Reappraisal*, 40(4) WC 536 (2017); Erik Hovenkamp, *Antitrust Policy for Two-Sided Markets*, https://ssrn.com/abstract=3121481; Lapo Filistrucchi, Damien Geradin, Eric van Damme & Pauline Affeldt, *Market Definition in two-sided Markets: Theroy and Practice*, 10(2) J. Competition L. & Econ. 293 (2014); Sebastian Wismer, Christhan Bongard & Arno Rasek, *Multi-Sided Market Economics in Competition Law*

Google's abusive conduct,[151] and what an appropriate implementation of the EU Comission's remedies would look like.[152]

Evidence in the case included 5.2 Terabytes of search result data from Google. However, judging from the publicly available information, the EU Commission does not seem to have had any special insight into the functioning of Google's search algorithms. In order to establish that Google's algorithms, including one called 'Panda', demoted competing shopping comparison services[153] according to certain criteria,[154] the EU Commission relied on blogposts and documents,[155] as well as the fact that the visibility (i.e. the rate of appearance and ranking on Google) of competing comparison shopping services was at the highest before the launch of Panda and dropped afterwards with no sustainable recovery.[156] The fact that Google Shopping was not subject to the same ranking mechanism as its competing services was apparently established based on emails, replies to the Commission's request for information, and other data.[157]

Nor does the Commission attempt to meddle, with the remedies it ordered, in the design or working of Google's search algorithm. The Commission stated, for instance, that 'the Monitoring Trustee's

Enforcement, 8(4) JECLAP 257 (2017); Gönenç Gürkaynak, Öznur İnanılır, Sinan Diniz & Ayşe Gizem Yaşar, *Multisided markets and the challenge of incorporating multisided considerations into competition law analysis*, 5(1) Journal of Antitrust Enforcement 100 (2017).

[151] For example, discrimination (cf. Anca Chirita, *Google's Anti-Competitive and Unfair Practices in Digital Leisure Markets*, 11(1) The Competition Law Review 109, 120, 122 (2015); Renato Nazzini, *Google and the (Ever-stretching) Boundaries of Article 102 TFUE* [sic], 6(5) JECLAP 301, 307-310 (2015)), tying (*pro*: Chirita, *id*., at 121; Benjamin Edelman, *Does Google Leverage Market Power Through Tying and Bundling?*, 11(2) J. Competition L. & Econ. 365, 369-378 (2015)), refusal to supply (*contra*: Chirita, *id*., 123; Nazzini, *id*., at 307-310), margin squeeze (contra: Nazzini, *id*., at 307-310) or lack of any abuse and theory (John Lang, *Comparing Microsoft and Google: The Concept of Exclusionary Abuse*, 39(1) WC 5, 27-28 (2016); Torsten Körber, *Common Errors Regarding Search Engine Regulation – and How to Avoid Them*, 36(6) ECLR 239 (2015)).

[152] The EU Commission specified the remedies in its corrected Tender Specification of 17 July 2017 for Technical Expertise in the case, 4-5, https://etendering.ted.europa.eu/cft/cft-documents.html?cftId=2629; *see* for case law on access remedies and Google's implementation: Bo Vesterdorf & Kyriakos Fountoukakos, *An Appraisal of the Remedy in the Commission's Google Search (Shopping) Decision and a Guide to its Interpretation in Light of an Analytical Reading of the Case Law*, 9(1) JECLAP 3 (2018); calling this a 'magic stroke' and favouring the EU Commission not to fumble with any algorithms: Rupprecht Podszun, *The Google case: First Comments by Haucap, Kersting, Podszun*, https://www.d-kart.de/the-google-case-first-comments.

[153] Google Search (Shopping), *supra* n. 148, at para. 349.

[154] Google Search (Shopping), *supra* n. 148, at para. 352.

[155] Google Search (Shopping), *supra* n. 148, at para. 358.

[156] Google Search (Shopping), *supra* n. 148, at para. 361.

[157] Google Search (Shopping), *supra* n. 148, at para. 380-383.

functions shall not include … the examination of Google's Web Search algorithms'[158] and that '[t]he objective of the Commission is not to interfere in Google's search algorithm'.[159] Subsequently, the proposed remedy of equal treatment[160] 'would not interfere with … the algorithms Google applies'[161] and '[t]he Commission Decision does not object to the design of Google's generic search algorithms or to demotions as such'.[162]

Regarding both evidence and remedies, the EU Commission's approach focussed – pointedly speaking – more on the market results of Google's conduct than on the (in)appropriateness of the algorithmic design which brought them about.

3.2[b] Lufthansa

In the context of the insolvency of Air Berlin, the German Bundeskartellamt started a preliminary investigation[163] to assess the initiation of proceedings against Lufthansa[164] due to abusive pricing.[165] After Air Berlin's insolvency, Lufthansa's algorithmically determined ticket fares skyrocketed (+ 25-30%) on certain – now monopolistic – routes.[166] In the end, the Bundeskartellamt did not initiate proceedings because, first, even after Lufthansa had increased its flight frequency and started using bigger airplanes, a capacity

[158] Commitments in Case COMP/C-3/39.740, 3 April 2013, Annex 4, Section A, para. 6, ec.europa.eu/competition/antitrust/cases/dec_docs/39740/39740_8608_5.pdf.
[159] EU Commission Statement on the Google investigation, 5 February 2014, http://europa.eu/rapid/press-release_SPEECH-14-93_en.htm.
[160] Cf. on this duty Eduardo Aguilera Valdiviva, *The Scope of the 'Special Responsibility' upon Vertically Integrated Dominant Firms after the Google Shopping Case: Is There a Duty to Treat Rivals Equally and Refrain from Favouring Own Related Business?*, 41(1) WC 43 (2018).
[161] Commission MEMO/15/4781, http://europa.eu/rapid/press-release_MEMO-15-4781_en.htm.
[162] Commission MEMO/17/1785, http://europa.eu/rapid/press-release_MEMO-17-1785_en.htm; Valdiviva, *supra* n. 160, at 66, argues this is because of Google's freedom to develop an editorial judgment.
[163] Bundeskartellamt, Press release of 29 May 2018, https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2018/29_05_2018_Lufthansa.html;jsessionid=1A8D22E0F52CCB06EEBABE068F36CB66.2_cid371?nn=3591568.
[164] Lufthansa-subsidiary Austrian Airlines might also be facing an inquiry involving pricing algorithms, https://kurier.at/wirtschaft/ueberteuert-behoerde-hat-fluege-wien-bruessel-im-visier/400051874.
[165] Interview with the president of the Bundeskartellamt Andreas Mundt with in Neue Osnabrücker Zeitung, http://www.bundeskartellamt.de/SharedDocs/Interviews/DE/2018/180127_NOZ.html.
[166] Bundeskartellamt, Press release of 29 May 2018, *supra* n. 163.

decline of 20% remained.[167] Second, due to easyJet's quick entry into the market, the price increase was not lasting.[168] Finally, the Bundeskartellamt held the view that it was mainly easyJet and not Lufthansa that moved into Air Berlin's market position which resulted in a market structure comparable to the one before Air Berlin's insolvency.[169]

Nonetheless, the case brings up the important question as to what extent the insolvency of a competitor – or similar changes in market structure – have to be considered in the price determination parameters of an algorithm and whether there is a duty to monitor and adjust (potentially after a grace period) the algorithm in the event of such structural changes. This issue gains in significance if insolvency leads to a dominant position of the remaining market participant, subjecting the latter to the stricter requirements for dominant companies. The Bundeskartellamt emphasized that the use of an algorithm does not exempt a company from its competition law responsibilities.[170] The somewhat simplistic wording of this statement may have been due to the fact that the algorithm at issue still required a great deal of human intervention.[171] In any case, companies with substantial market shares are well advised to monitor their market position and, in case of their exceeding the threshold for market dominance, to undertake the necessary adjustments from an antitrust perspective.

3.3. Data protection violations as anticompetitive behaviour?

In March 2016, the Bundeskartellamt initiated proceedings against Facebook, investigating whether Facebook's terms of service regarding user data do not only violate data protection law but also abuse a dominant position by imposing unfair conditions on Facebook users.[172] According to the authority's preliminary assessment,

---

[167] Bundeskartellamt, Fallbericht B9-175/17 – *Lufthansa*, 3, https://www.bundeskartellamt.de/SharedDocs/Entscheidung/DE/Fallberichte/Missbrauchsaufsicht/2018/B9-175-17.pdf?__blob=publicationFile&v=4.

[168] Bundeskartellamt, Press release of 29 May 2018, *supra* n. 163.

[169] Bundeskartellamt, Fallbericht B9-175/17 – *Lufthansa*, *supra* n. 167, at 3.

[170] 'The answer seems simple: companies cannot hide behind algorithms that they use, and in the meantime Lufthansa has acknowledged this' (Andreas Mundt, *Sixty years and still exciting – the Bundeskartellamt in the digital era*, 6(1) JAE 1, 3 (2018)).

[171] '*[T]he airlines specify the framework data and set the parameters for dynamic price adjustment separately for each flight. The airlines also actively manage changes to these framework data and enter unanticipated events manually, which are not automatically accounted for by the system*' (Bundeskartellamt, Press release of 29 May 2018, *supra* n. 163).

[172] Bundeskartellamt, press release of 2 March 2016, https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/201

Facebook is, in fact, dominant in the (German) market for social networks.[173] As to abuse, '[t]he authority holds the view that Facebook is abusing this dominant position by making the use of its social network conditional on its being allowed to limitlessly amass every kind of data generated by using third-party websites and merge it with the user's Facebook account. These third-party sites include firstly services owned by Facebook such as WhatsApp or Instagram, and secondly websites and apps of other operators with embedded Facebook APIs'.[174] 'If a third-party website has embedded Facebook products such as the "like" button or a "Facebook login" option or analytical services such as "Facebook Analytics", data will be transmitted to Facebook via APIs the moment the user calls up that third party's website for the first time. These data can be merged with data from the user's Facebook account, even if the user has blocked web tracking in his browser or device settings'.[175] 'Participation in Facebook's network is conditional on registration and unrestricted approval of its terms of service. Users are given the choice of either accepting the "whole package" or doing without the service … According to the Bundeskartellamt's preliminary assessment, Facebook's terms of service are at least in this aspect inappropriate'[176] – as exploitative business terms[177] – 'and violate data protection provisions to the disadvantage of its users. In view of the company's dominant position, it can also not be assumed that users effectively consent to this form of data collection and processing'.[178] Regarding the theory of harm (economically) legitimizing its intervention, the Bundeskartellamt realizes the need to develop a creative approach as Facebook's services are for free and the company's (potentially) exploitative business terms do not, therefore, inflict direct financial losses on Facebook users.[179] However, the Bundeskartellamt says,

6/02_03_2016_Facebook.html?nn=3591568; cf. also Robert McLeod, *Novel But a Long Time Coming: The Bundeskartellamt Takes on Facebook*, 7(6) JECLAP 367 (2016).

[173] Bundeskartellamt, Preliminary assessment in Facebook proceeding, 19 December 2017, https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2017/19_12_2017_Facebook.html?nn=3591568.; for details, cf. Bundeskartellamt, Background information on the Facebook proceeding, 19 December 2017, 3, https://www.bundeskartellamt.de/SharedDocs/Publikation/EN/Diskussions_Hintergrundpapiere/2017/Hintergrundpapier_Facebook.pdf?__blob=publicationFile&v=6.

[174] Bundeskartellamt, Preliminary assessment in Facebook proceeding, *supra* n. 173. API stands for 'application programming interface' and consists of building blocks that a programmer can use to more easily create a computer program.

[175] Bundeskartellamt, Background information on the Facebook proceeding, *supra* n. 173, at 2.

[176] Bundeskartellamt, Preliminary assessment in Facebook proceeding, *supra* n. 173.

[177] Bundeskartellamt, Background information on the Facebook proceeding, *supra* n. 173, at 4.

[178] Bundeskartellamt, Preliminary assessment in Facebook proceeding, *supra* n. 173.

[179] Bundeskartellamt, Background information on the Facebook proceeding, *supra* n. 173, at 4.

'[t]he damage for the users lies in a loss of control: they are no longer able to control how their personal data are used. … Facebook's merging of the data thus also constitutes a violation of the users' constitutionally protected right to informational self-determination'.[180]

A core, and novel, feature of the Facebook case consists in a very close interaction between data protection law and competition law. According to the concept of the Bundeskartellamt, algorithmic data collection and data processing that violate (digital) data protection provisions can result in a breach of the obligations competition law imposes on dominant undertakings. This is the case because – in the authority's words – '[w]here access to the personal data of users is essential for the market position of a company, the question of how that company handles the personal data of its users is no longer only relevant for data protection authorities. It becomes a relevant question for the competition authorities, too. … In the digital economy, the collection and processing of data is an entrepreneurial activity that has great relevance for the competitive performance of a company. The legislator has acknowledged this relevance and in § 18(3a) of the German Competition Act made access to personal data a criterion for market power, especially in the case of online platforms and networks'.[181] Moreover, the authority considers data protection 'principles' instructive on whether Facebook's terms and conditions are exploitative in a competition law sense.[182] 'In its assessment the Bundeskartellamt includes the principles of the harmonised European data protection rules, in particular the EU General Data Protection Regulation (GDPR), which will enter into force in May 2018, but also the currently applicable 95/46 EC Data Protection Directive, which can be directly applied to cases under § 19(1) GWB'.[183] 'Monitoring the data processing activities of dominant companies is … an essential task of the competition authority which cannot be fulfilled by a data protection authority … For this purpose, the Bundeskartellamt works closely with data protection authorities'.[184] Confident as these statements sound, the combined application of competition and data protection law and the delineation of the respective agencies'

[180] Bundeskartellamt, Background information on the Facebook proceeding, *supra* n. 173, at 4.
[181] Bundeskartellamt, Background information on the Facebook proceeding, *supra* n. 173, at 1-2.
[182] Bundeskartellamt, Background information on the Facebook proceeding, *supra* n. 173, at 4.
[183] Bundeskartellamt, Background information on the Facebook proceeding, *supra* n. 173, at 5-6.
[184] Bundeskartellamt, Background information on the Facebook proceeding, *supra* n. 173, at 2.

purviews pose considerable challenges. Hence, it comes as no surprise that the Bundeskartellamt's approach is controversial.[185]

3.4. Further constellations

The selected case-law presented here does, of course, not comprise all problematic settings that present algorithmic markets, let alone their development towards the use of ever more complex, self-learning and 'intelligent' technology may pose. Access for competitors to superior algorithmic/AI-tools; dynamic, personalized pricing;[186] more generally, many-facetted discrimination resulting from the economically rational and statically efficient (inter)actions of algorithmic business agents; new types of merger control remedies addressing, for instance, impediments to competition resulting from the merger of big data portfolios[187] and algorithmic infrastructure or the divestiture of AI-systems and the know-how they embody – these are among the constellations likely to keep competition authorities busy in the future. What can the present algorithm-related case-law and the look at other legal areas contribute to preparing competition law enforcement for these challenges?

[185] Contra: Marixenia Davilla, *Is Big Data a Different Kind of Animal? The Treatment of Big Data Under the EU Competition Rules*, 8(6) JECLAP 381 (2017); advocating a holistic approach between competition, consumer and data protection law: Wolfang Kerber, *Digital Markets, Data, and Privacy: Competition Law, Consumer Law, and Data Protection*, 11(11) JIPLP 856, 865-866 (2016); pro: Giulia Schneider, *Testing Art. 102 TFEU in the Digital Marketplace: Insights from the Bundeskartellamt's investigation against Facebook*, 9(4) JECLAP 213, 214, 225 (2018).

[186] It could be argued that Art. 22 GDPR already establishes a duty to inform about personalized pricing because profiling concerns data about someone's economic situation, cf. Art. 4(4) and Recital 71; see Maurits Dolmans, *Artificial Intelligence and the Future of Competition law – Further Thoughts*, Presentation from 2 May 2017, slide 20, https://www.coleurope.eu/sites/default/files/uploads/event/dolmans.pdf; Michal Gal argues that from an antitrust perspective, it is harder that companies coordinate dynamic pricing unless there are division agreements or the same data pool is being used (Caron Beaton-Wells, *supra* n. 116, https://overcast.fm/+N2zZD5F3Q/35:04); the Competition and Markets Authority concludes that explicit collusion and personalized pricing are compatible but unlikely to occur together, tacit coordination, on the other hand, and personalized pricing very unlikely to occur together, Competition and Markets Authority, *supra* n. 140, at para. 7.31-7.44.

[187] Arguing, however, against special treatment of big data under the EU competition law framework: Davilla, *supra*. n. 185.

4. Where competition law might learn and improve

Among the many lessons and proposals for the development of competition law that one might draw from the previous sections of this contribution, we want to highlight the following:

(1) Competition authorities ought to improve the **factual and analytical foundation** on which they base their decisions and policies.[188] This suggests not only additional inquiries into sectors on which digitalization and 'algorithmization' have a strong impact.[189] MiFID II,[190] for instance, shows that algorithm users' duties to inform and document can contribute a lot to keeping authorities (at least theoretically) up-to-date. When specific issues arise, authorities should be able and willing to carry out – be it alone or in cooperation with the involved undertakings – 'sandboxing' exercises, i.e. the testing of algorithms or AI systems in a protected model environment.[191] Some suggest, inter alia with regard to Swiss competition law,[192] that firms may submit their algorithms to the respective competition law authority for analysis and clearance.[193] A

[188] Rupprecht Podszun, *The More Technological Approach: Competition Law in the Digital Economy*, 101, 107 (Gintarė Surblytė, Competition on the Internet, Springer 2015); cf. Monopolkommission, Hauptgutachten 2018, *supra* n. 122, at para. 240; the German Bundeskartellamt and the French Autorité de la concurrence launched a joint project on algorithms and their implications on competition aiming at analyzing challenges resulting from algorithms and trying to identify any approaches, https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2018/19_06_2018_Algorithmen.html?nn=3591568.

[189] Cf. Monopolkommission, Hauptgutachten 2018, *supra* n. 122, at para. 233-237, also evaluating the right of consumer protection organisations to request sector inquiries by amending § 34a of the German Act against Restraints of Competition (Competition Act – GWB).

[190] Cf. *supra* section 2.1.

[191] Cf. *supra* section 2.3 under 'testing and monitoring'.

[192] Picht & Freund, *supra* n. 109, at 408.

[193] The FTC, for instance, established the Office of Technology Research and Investigation (https://www.ftc.gov/about-ftc/bureaus-offices/bureau-consumer-protection/office-technology-research-investigation) that will also play an important role in helping the FTC understand how algorithms and AI software work in particular markets (remarks of former FTC Commissioner Terrell McSweeny, Algorithms and Coordinated Effects, University of Oxford Center for Competition Law and Policy, May 22, 2017, 6, https://www.ftc.gov/system/files/documents/public_statements/1220673/mcsweeny_-_oxford_cclp_remarks_-_algorithms_and_coordinated_effects_5-22-17.pdf); similarly, to deal with algorithms, AI and big data, the UK's competition and Markets Authority is building a technology team (https://www.ft.com/content/349103ba-c631-11e7-b2bb-322b2cb39656; https://www.gov.uk/government/news/cma-appoints-stefan-hunt-to-top-digital-role). It even declared: 'Competition authorities and regulators can and do use algorithms to detect cartels. The CMA has created a cartel screening tool to help procurers screen their tender data for signs of cartel behaviour. This software looks at factors including the text of the bids. It is unlikely the features of collusion relevant to

positive result of such an 'ex-ante audit' could mitigate the risk of being sanctioned for unwanted effects the respective algorithms generate when used in a real-world environment. This option may be particularly attractive regarding 'black box algorithms' whose reactions to complex settings are difficult to predict.[194]

(2) Customers can have great difficulties deciphering complex algorithmic market conduct, detecting practices harmful to them, and defending their interests against such practices. A healthy level of **private** competition law **enforcement**[195] – especially for stand-alone cases without prior competition authority proceedings – may therefore require specific **customer information rights**,[196] keyed to customers' comprehension and resources, thereby enabling them to effectively protect their interests.

(3) Competition on digital markets is, as yet, less well understood than competitive processes on more traditional, 'brick-and-mortar' markets, it is rapidly changing and these characteristics will last well into the future. Besides addressing anticompetitive behaviour ex post, competition authorities should therefore strengthen their **ex-ante monitoring**[197] of digital markets, in particular regarding undertakings which have already violated competition law and subsequently altered their algorithmic conduct in order to (purportedly) terminate the violation. Such preventive monitoring should, however, not gravitate towards a – highly impracticable and anti-innovative – scenario in which new algorithms or AI systems (legally or factually) require ex-ante authorization to be put on the market.[198]

(4) To perform the increased analytical and monitoring activities sketched above, competition authorities need **additional resources** (know-how, tools, skilled staff, etc.).[199] In the

---

comparing detailed tenders to prevent bid-rigging will be useful in identifying price fixing tacit coordination collusion in online retail markets' (Competition and Markets Authority, *supra* n. 140, fn. 22); *see also* Schwalbe, *supra* n. 140, at 22; *infra* n. 199.

[194] OECD, *supra* n. 4, at 47-48.

[195] This includes the private enforcement of rules against unfair competition.

[196] Cf. *supra* section 2.3 under 'transparency'.

[197] Cf. *supra* section 2.3 under 'testing and monitoring'.

[198] Google for example, changes its algorithm 500-600 times each year, https://moz.com/google-algorithm-change.

[199] Cf. also s*upra* n. 193; in Switzerland, the Competition Commission has mentioned the possibility to employ technical specialists (https://www.nzz.ch/wirtschaft/das-anliegen-der-fair-preis-initiative-ist-berechtigt-ld.1391008) and is at least building on its technical expertise (https://www.nzz.ch/wirtschaft/wenn-algorithmen-kartelle-bilden-ld.1415028); Margrethe Vestager publicly discussed employing algorithms to detect collusion

aftermath of the Google Search (Shopping) decision, for instance, the EU was looking for a technical expert[200] to monitor compliance with and implementation of the decision.[201] The expert's tasks were rather challenging and included the assessment – depending also on Google's means of implementation of the remedy – of 'the processes and methods deciding the positioning and display of Google's comparison shopping service, as well as of competing comparison shopping services in Google's general search results pages in response to a query, including relevance standards, ranking algorithms, adjustment or demotion mechanisms and their respective conditions, parameters and/or signals'.[202]

(5) The complex and rapidly changing nature of algorithmic conduct and markets suggests a '**results-based approach**'[203] which entitles authorities to intervene where they detect anticompetitive market outcomes, even if they do not (immediately) manage to prove flaws in algorithmic design or the presence of subjective elements, such as knowledge or intention.[204] In fact, this may constitute a viable long-term strategy for competition authorities in the digital era. However, as the results of complex, even self-learning algorithms and their interactions with other (algorithmic) market forces can be very hard for undertakings to predict and control,[205] a results-based approach may generate excessively strict liability absent limiting

(https://www.reuters.com/article/us-eu-antitrust-algorithm/eu-considers-using-algorithms-to-detect-anti-competitive-acts-idUSKBN1I5198; Michal Gal is suggesting that competition authorities build on technical expertise, also considering that possible remedies may include orders to stop using the algorithm (altogether or only part of it), to not disclose the algorithm to competitors or to amend the algorithm (Caron Beaton-Wells, *supra* n. 116, https://overcast.fm/+N2zZD5F3Q/58:04).

[200] *See* https://ted.europa.eu/TED/notice/udl?uri=TED:NOTICE:244258-2017:TEXT:EN:HTML&tabId=1.

[201] *See* Tender Specifications, corrected version of 17 July 2017, 3, https://etendering.ted.europa.eu/cft/cft-document.html?docId=27867.

[202] *Id.*, at 6.

[203] Cf. also Gal, *supra* n. 141, at 44: 'Furthermore, the digital world increases the Paradox of Proof, in that market conditions make it easier to coordinate, and at the same time make it more difficult to prove the existence of an explicit agreement given that explicit inter-firm communication may be less essential. This suggests that, while the danger of harm might increase, it might also be less likely to find strong evidentiary inferences of an agreement. It is thus be time to rethink our laws and focus on reducing harms to social welfare rather than on what constitutes an agreement. There may well be a case for not binding ourselves to past formulations which no longer fit economic realities. In particular, the time may be ripe to reconsider prohibiting any conduct with potential anticompetitive tendencies, with no offsetting pro-competitive ones, even where such conduct does not constitute an agreement in the traditional sense.'

[204] Picht & Freund, *supra* n. 109, at 408.

[205] Monopolkommission, Hauptgutachten 2018, *supra* n. 122, at para. 170; Picht & Freund, *supra* n. 109, at 408.

concepts such as a predictability defense, a 'notice and re-adjustment' mechanism, or an exculpatory defense where an algorithm was designed according to due diligence procedures.[206] At the very least, authorities must consider such factors in their sanction regimes. At the same time, clearly undue conduct with regard to monitoring one's own algorithms, informing correctly about them, and reacting to perceivable anticompetitive results of their operations should loom large among the factors triggering (severe) competition law sanctions.

(6) **Compliance by default and by design** can serve as a policy element complementary to a results-based approach. The GDPR concept of privacy by design (Art. 25 para. 1 GDPR) requires companies to implement technical and organizational measures at the earliest stages of design in such a way that privacy and data protection principles are safeguarded right from the start. EU Commissioner Vestager advocated this standard of conduct for competition law as well, stating that '[w]hat businesses can – and must – do is to ensure antitrust compliance by design. That means pricing algorithms need to be built in a way that doesn't allow them to collude. Like a more honourable version of the computer HAL in the film *2001*, they need to respond to an offer of collusion by saying "I'm sorry, I'm afraid I can't do that".'[207] Indeed, undertakings should structure their digital tools in a way that promises these tools to operate in a procompetitive manner (procompetitiveness by design). Furthermore, the most procompetitive configuration of a tool should form the pre-installed standard configuration (procompetitiveness by default).[208] Some authors suggest that, regarding simple pricing algorithms, this may mean that the algorithms ought to be set not to react to price changes when they result from certain companies[209] or not to follow and match price *increases* by

[206] Nicolo Zingales, *Google Shopping: beware of 'self-favouring' in a world of algorithmic nudging*, https://www.competitionpolicyinternational.com/google-shopping-beware-of-self-favouring-in-a-world-of-algorithmic-nudging.

[207] This quote was preceded by the following remarks: 'And I think the EU's new rules on data protection, which will come into force next year, give us valuable ideas about how we can face that challenge. The concept of "data protection by design" makes clear that people's privacy can never be an afterthought. It has to be built into the way that services work from the very start. That's also how businesses need to think when they design and use algorithms. They may not always know exactly how an automated system will use its algorithms to take decisions', https://ec.europa.eu/commission/commissioners/2014-2019/vestager/announcements/bundeskartellamt-18th-conference-competition-berlin-16-march-2017_en.

[208] Privacy by default (Art. 25 para. 2 GDPR) requires companies to process personal data with the highest privacy protection in a way that by default personal data is not accessible to an indefinite number of persons.

[209] Antonio Gomes, *Disruptive Innovation, Big Data and Algorithms*, OECD Presentation of 31 August 2017, slide 40,

competitors but only their price decreases.[210] Others, like the German Monopolies Commission, point to the risk that very rigid regulatory stipulations may block legitimate algorithmic pricing strategies and create barriers to market entry by raising regulatory costs.[211] The OECD mentions regulatory intervention by way of rules on algorithm design, preventing, for instance, algorithms from reacting to features or variables necessary for tacit collusion. However, the OECD underlines also that such rules place considerable supervising burdens on agencies.[212] The really intricate step is, in any case, to identify what the design and the default should be in complex scenarios. The design of regulatory stipulations for pricing algorithms will be particularly challenging with regard to deep learning algorithms that are not supposed to follow an immutable, pre-programmed pricing pattern. Sometimes, previous experience will tell that a particular setting has a tendency to produce non-compliant results and that it should, therefore, *not* be the design and default. Sometimes, economic theory or sandbox exercises[213] will be capable of singling out design/default-worthy configurations, although the growing complexity of (the interactions of) algorithmic/AI systems tends to complicate such predictions. Standard setting[214] may, in some instances, define compliant configurations that can serve as a reference point for both undertakings and authorities. Where previous experience, clear results from testing or theory, convincing standards or similar guidance is not at hand, though, competition law enforcement must be careful not to place excessive liability burdens on the market players[215] by considering every undesirable market outcome as the result of a design/default violation.

(7) The compensatory and, in particular, the steering purpose of competition law's liability rules depend not least on the clear distribution of responsibilities among the involved players. In the digital world, characteristic facets of this challenge are the

http://www.sic.gov.co/sites/default/files/documentos/092017/antonio-ferreira-gomes-disruptive-innovation-big-data-and-algorithms.pptx.

[210] Paolo Siciliani, *Tackling Algorithmic-Faciliated Tacit Collusion in a Proportionate Way*, JECLAP 1, 2 (forthcoming); identifying this as a topic for further research while also pointing out that the underlying rationale of maximizing firm profit might make this 'too interventionist and damage the competitive process to restrict firms' ability to set its own prices', Competition and Markets Authority, *supra* n. 140, at para. 9.1(b).

[211] Monopolkommission, Hauptgutachten 2018, *supra* n. 122, at para. 251; cf. also Gomes, *supra* n. 209, slide 40.

[212] OECD, *supra* n. 4, at 50.

[213] Cf. *supra* section 2.3 under 'testing and monitoring'.

[214] Cf. *supra* section 2.3 under 'standard setting'.

[215] Zingales, *supra* n. 206.

liability distribution between developers, implementers,[216] and users of algorithms/AI systems,[217] especially where developer and implementer do not belong to the same company and where users engage not merely in passive consumption but also in active configuration or even co-shaping activity. Competition law has yet to get down to the nitty-gritty of appropriate liability rules for these relationships. Monitoring obligations for developers may be a helpful element of such rules, especially where a developer caters to numerous implementers and gains, therefore, a bird's-eye view on the issues its algorithms/AI systems may raise. Some propose that digital platforms establishing a marketplace should be requested to oversee or even limit the pricing conduct of their market participants, for instance by built-in delays for price changes to go live or by allowing price changes only every couple of days.[218] Incentivizing parties to clearly document who decided on the specifications for a system may be worthwhile as well, for instance by granting developers a 'client's choice defence' if an (anticompetitive) setting was requested by the implementer. To avoid effective sanctioning – especially in high-damage private enforcement cases – to be undercut by the (intentional) insolvency of small algo-developers, a subsidiary liability of implementers could incentivize them to request that developers take solvency measures.

(8) As in other areas which display(ed) rapid technological progress and a strong potential for further innovation, protecting the **dynamic efficiency** of algorithmic/AI markets becomes both a major and a difficult task for competition law.[219] Everybody wants innovation but nobody is – or will ever be – able to designate the mathematical formula for calculating which forms of market structure and conduct yield the best innovation results. Nonetheless, competition law must neither disregard dynamic efficiency nor turn it into an unspecific knockout argument for justifying whatever option decision-makers prefer. Instead, competition law and practice must keep working on concretisations of the innovation paradigm which provide guidance in concrete cases. To propose examples, a very strict liability for anticompetitive outcomes in complex algorithmic markets, detailed and inflexible requirements for the design of algorithms/AI systems, as well as micro-managing remedies are

[216] Cf. Monopolkommission, Hauptgutachten 2018, *supra* n. 122, at para. 215, according to which algorithms represent the prior will of the user but a shift in liability may have to be considered regarding self-learning algorithms.
[217] Monopolkommission, Hauptgutachten 2018, *supra* n. 122, at para. 252-273.
[218] Siciliani, *supra* n. 210, at 4.
[219] *See also* Podszun, *supra* n. 188, at 108.

likely to be more of a hindrance than a help for the dynamic efficiency of the affected markets.

5. Conclusion and outlook: The interaction between competition law and other (regulatory) areas of the law

The increase of algorithmic and – in the future – of AI-based market conduct impacts competition in ways the case-law reflects today and in ways we do not yet perceive. To defend competition against the negative part of this impact, competition law and enforcement must develop in some respects. The experiences and rules made by other areas of the law can help to guide this process. We have taken a closer look at data protection law and financial markets regulation, but these are by far not the only relevant fields. One trend goes towards the setting of ethical rules for AI.[220] Although not addressed in detail here, rules against unfair competition are another major element, both as a template for and a tool complementary to the provisions against cartels and abuse of dominance. Dynamic and/or individualized pricing, for instance, may well be a type of conduct to be addressed more appropriately by unfair competition rules than by other parts of competition law.[221]

At the same time, thinking about a competition law for the digital era raises the question of how this competition law ought to interact with neighbouring areas of the law which also claim to set rules for the digital world. The present contribution cannot go on to analyse this complex interplay in detail, but it proposes four theses which, hopefully, help to fuel future research and discussion:

(1) **Competition law and enforcement should stand back** if and insofar another set of rules exists/evolves that provides an appropriate legal framework for the algorithmic/AI-economy. Such a framework must safeguard the protective purposes of competition law, as well as effective enforcement.

[220] *See* for example http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P8-TA-2017-0051&language=EN&ring=A8-2017-0005#BKMD-12; http://standards.ieee.org/develop/indconn/ec/ead_v1.pdf; https://futureoflife.org/ai-principles; https://www.partnershiponai.org; https://cyber.harvard.edu/topics/ethics-and-governance-ai.

[221] Cf. Florent Thouvenin, *Dynamische Preise, Eine Herausforderung für das Datenschutz-, Wettbewerbs- und Vertragsrecht*, Jusletter IT 22 September 2016, para 29-46; Picht & Freund, *supra* n. 109, at 407: 'algorithm-based individual price differentiation is—so far—something like a "Loch Ness Monster", often conjured-up but rarely, if ever, reliably detected'; the Competition & Markets Authority, did not find much evidence of it in practice either; cf. in detail: Competition and Markets Authority, *supra* n. 140, para. 7.7-7.26 & Annex I, esp. para. 1 and 17.

(2) At present, however, **neither** competition nor any other **area of the law** seem **optimally equipped** to address the issues arising from algorithms and AI.[222]

(3) If areas other than competition law undertake to tackle the new issues, they ought to strive for rules that **sync with competition law**. In case they are intended to derogate competition law, these rules must incorporate competition law's protective purposes.

(4) Where competition law needs to intervene, it must be enabled to do so appropriately and effectively. This is where the tools discussed in section 4 come into play. Even using them, '[c]ompetition rules can't solve every problem on their own. But they can make an important contribution to keeping digital markets level and open'.[223]

(5) A stand-alone, all-encompassing and fine-meshed regulatory framework for AI and algorithmic market activity should – although proposed by some scholars[224] – not be implemented at present.[225] Sufficient empirical data and experience on which to base such legislation are, as yet, not available. Furthermore, trying to cover all pertinent legal concerns and legitimate party interests in a single regulatory act seems, to say the least, demanding. Undertaking, under the present circumstances, sweeping regulation risks generating incoherencies, hindering innovation[226] as well as the market entry of new players, and

[222] Cf. *supra* section 3.

[223] Margrethe Vestager's speech in Munich on Competition in a big data world, https://ec.europa.eu/commission/commissioners/2014-2019/vestager/announcements/competition-big-data-world_en.

[224] Gawer, for instance, suggests the creation of an independent digital regulator coordinating and supervising aspects of internet and data, *see* Annabelle Gawer, *Competition Policy and Regulatory Reforms for Big Data: Propositions to Harness the Power of Big Data while Curbing Platforms' Abuse of Dominance*, note submitted to the hearing on Big Data of the 126th meeting of the OECD Competition Committee, https://one.oecd.org/document/DAF/COMP/WD(2016)74/en/pdf; Scherer proposes enacting an Artificial Intelligence Development Act (AIDA) which would give an agency the competence to certify AI systems with the consequence of limited tort liability for certified programs compared to strict joint and several liability for uncertified programs, *see* Matthew U. Scherer, *Regulating Artificial Intelligence Systems: Risks, Challenges, Competencies, and Strategies*, 29(2) Harv. J.L. & Tech. 354, 353-400 (2016), http://jolt.law.harvard.edu/articles/pdf/v29/29HarvJLTech353.pdf.

[225] Cf. also the relatively conservative approach of the OECD, *supra* n. 4, at 50.

[226] For instance, the development of new, desirable algorithmic tools, cf. OECD, *supra* n. 4, at 47; cf. also Vlad Dan Roman, *Digital Markets and Pricing Algorithms – a Dynamic Approach Towards Horizontal Competition*, 39(1) ECLR 37, 44 (2018); FTC Chairman Maureen Ohlhausen with regards to net neutrality regulation: '[i]*n dynamic, innovative industries like internet services, an ex post case-by-case enforcement-based approach has advantages over ex ante prescriptive regulation. It mitigates the regulator's knowledge problem and allows legal principles to evolve*

resulting in a body of law that needs continuous maintenance and adjustments. Although it may seem less appealing at first sight, an evolutionary approach that moves step-by-step, using and harmonizing various complementary areas of the law may prove the wiser way of framing our digital future.

incrementally. A case-by-case approach also focuses on actual or likely, specifically-pled harms rather than having to predict future hypothetical harms' (https://www.ftc.gov/system/files/documents/public_statements/1231563/mko_rif_comment_7-17-2017_final.pdf).